2010 UBO/UBU Conference

Health Budgets & Financial Policy

Briefing: **HIPAA Scenarios – The MTF's Role in Protecting PHI**

Date: **25 March 2010**

Time: **0900 – 0950**

Objectives

- Recognize the role of TMA's Privacy Office in your day-to-day operations
- Understand the privacy laws, regulations, and policies that apply to MTF billing offices
  - New law/regulations in effect just this year
- Know your role in the privacy process
- Know what to do if a breach occurs

TMA Privacy Office

- Oversees protection of
  - Personally identifiable information (PII)
  - Protected health information (PHI)
- Works to ensure compliance with
  - Federal privacy and security laws
  - DoD regulations and guidelines
- Develops applicable DoD policies in compliance with federal law

TMA Privacy Office

- Manages and evaluates potential risks and threats to privacy and security
  - HIPAA Security Risk assessments
  - Internal Privacy Office compliance assessments
- Establishes organizational performance metrics to identify and measure potential compliance risks
- Engages TMA stakeholders in the process of protecting privacy
  - Education and awareness materials
  - Training

Definitions

Definitions

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information that is linked or linkable to an individual

Source: DoD 5400.11-R, "DoD Privacy Program", May 14, 2007

Definitions

Protected Health Information (PHI): Individually identifiable information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to:

- The past, present, or future physical or mental health, or condition of an individual
- Provision of health care to an individual
- Payment for the provision of health care to an individual

If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered PHI.

Source: DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003

Electronic Protected Health Information

- Electronic Protected Health Information (ePHI): Any PHI that is created, stored, transmitted, or received electronically on any medium, including:
  - Personal computers with their internal hard drives used at work, home, or traveling
  - External portable hard drives, including iPods
  - Magnetic tape or disks
  - Removable storage devices, such as USB portable memory drives/keys, CDs, DVDs, and floppy disks
  - PDAs, Smartphones
  - Electronic transmission includes data exchange (e.g., e-mail or file transfer) via wireless, Ethernet, modem, DSL, or cable network connections

Examples of PII/PHI

Personally Identifiable Information (PII)

Information that can be used to distinguish or trace an individual's identity, including personal information that is linked or linkable to a specified individual

Protected Health Information (PHI)

Information that is created or received by a Covered Entity and relates to the past, present, or future physical or mental health of an individual; providing or payment for healthcare to an individual; and can be used to identify the individual

- Name
- Social Security Number
- Age
- Date and place of birth
- Mother's maiden name
- Biometric records
- Marital status
- Military Rank or Civilian Grade
- Race
- Salary
- Home/office phone numbers
- Other personal information which is linked to a specific individual (including Health Information)
- Electronic mail addresses
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address
- Claim form
- Electronic claim form
- Payment history
- Account number
- Name and address of health care provider
- Diagnosis
- Number of years of military service*

* Combining number of years with rank can

PII/PHI Data

- The sensitivity of data is important to determine the level of protection and privacy required
- Data may include Personally Identifiable Information (PII) and Protected Health Information (PHI)
- Even a small amount of PHI or PII can be used to determine an individual's identity
- The definition of data includes paper-based records as well as electronic media

De-Identified PHI

De-identified PHI is data that ***excludes*** the following **18** categories of direct identifiers of the individual or of relatives, employers, or household members of the individual:

De-Identified PHI	
▪ Names ▪ All geographic subdivisions smaller than a State ▪ All elements of dates (except year) ▪ Telephone numbers ▪ Fax numbers ▪ Electronic mail addresses ▪ Social Security Numbers ▪ Medical Record numbers ▪ Account numbers ▪ Health plan beneficiary numbers ▪ Certificate or license numbers	• Internet protocol (IP) address • Device identifiers and serial numbers • Web universal resource locators (URLs) • Biometric identifiers, including finger and voice prints • Vehicle Identification Numbers and License Plate Numbers • Full-face photographic images and comparable images • Any other unique, identifying characteristic or code, except as permitted for re- identification in the HIPAA Privacy Rule

PII/PHI Data

Only PII and PHI are protected by the Privacy Rule. Data that is de-identified is not protected by the Privacy Rule.

No restrictions on using de-identified health information.

It does not identify or provide a reasonable basis to identify an individual.

2 ways to de-identify information:

1. Using statistics or
2. Removing specific identifiers

Policy

Privacy-Related Legislation

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Privacy placeholder was inserted at the last minute
  - Since Congress did not pass follow-on legislation, the Administration issued regulations

Privacy-Related Legislation

- American Recovery and Reinvestment Act of 2009 (ARRA) [AKA Stimulus Package]
  - Health Information technology for Economic and Clinical Health Act (HITECH Act)
    - EHR Incentive Program (meaningful use of EHR technology)
    - Standards, implementation specifications, certification criteria for EHR technology
    - Additional privacy and security protections

TMA Guidance Documents

- 5 June 2009 Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)
  - Privacy and security training and communication must be, “job-specific and commensurate with an individual’s responsibilities”
  - Training must be a “prerequisite before an employee, manager, or contractor is permitted to access DoD systems”
  - Encompasses a general orientation, specialized training, management training, and Privacy Act System of Records Training along with annual refresher training

Identity Theft Risk Analysis

- 5 factors “to consider when assessing the likelihood of risk and/or harm”
  - (1) Nature of the data elements breached
  - (2) Number of individuals affected
  - (3) Likelihood the information is accessible and usable
  - (4) Likelihood the breach may lead to harm
  - (5) Ability of the agency to mitigate the risk of harm

TMA Guidance Documents

Policy implements May 2007 OMB Memo

- 4 general areas all federal agencies were required to address:
  (1) Safeguarding Against the Breach of PII
  (2) Incident Reporting and Handling Requirements
  (3) External Breach Notification
  (4) Rules and Consequences (a new OMB requirement)

TMA Guidance Documents

OMB definition of breach

- Loss of control, compromise, unauthorized disclosure, unauthorized acquitting, unauthorized access or any similar term referring to situations where persons other than authorized users for an other than authorized purposes have access or potential access to personally identifiable information, whether physical or electronic

TMA Guidance Documents

- ASD/HA Memo, “Breach Notification Reporting for the Military Health System,” September 24, 2007
  - Establishes requirements for incident reporting by all components of the MHS
  - Requires that Services must contact the TRICARE Management Activity Privacy Office whenever data involving MHS beneficiaries’ PII is lost, stolen, or compromised

TMA Guidance Documents

- DoDI 6025.18 – Privacy of Individually Identifiable Health Information in DoD Health Care Programs
  - Was originally a Directive (6025.18)
  - Establishes policy and assigns responsibilities to implement standards for privacy of individually identifiable health information

TMA Guidance Documents

- DoD 6025.18-R, “DoD Health Information Privacy Regulation” (currently under revision)
  - Implements the HIPAA Privacy Rule throughout DoD
  - Defines the baseline health information privacy requirements for use of PHI regarding covered entities and business associate agreements
  - This Regulation is under revision

TMA Guidance Documents

- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
  - Establishes new requirements for reporting security breaches
  - Enhances requirements for safeguarding, collecting, and accessing Personally Identifiable Information
  - Provides guidelines for maintaining a system of records or a portion of a system of records when storing, processing, or transmitting PII
  - Outlines procedures for disclosure of personal information to and from third party agencies

Complying with the Rules

Access to PII/PHI

- Your staff may have access to all categories of PII/PHI. All PII/PHI must be handled with the appropriate level of care and protection.
- BUT access should be restricted to what is necessary to complete a work-related duty or job.
  - This "**minimum necessary standard"** is based on the *need to know* and the need to perform assigned duties and responsibilities.

Access to PII/PHI

- The minimum necessary standard does not apply to the following:
  - Disclosures to or requests by a healthcare provider for treatment.
  - Uses and disclosures made to the individual.
  - Uses and disclosures made after an individual's authorization has been granted.
- *If using a DoD information system with access to PII/PHI, security and awareness training must be completed prior to account set-up.*

Guidelines for PII/PHI

- Know what PII/PHI is available in your environment and how it can be accessed
  - Know how and where hard copy files are stored
  - Create and maintain an inventory of all documents that contain PII/PHI
  - Keep a list of employees who have access to PII/PHI – paper and electronic
- Control how much PII/PHI is maintained in your area
  - Limit the amount of PII/PHI to what is needed to reduce the risk of information being used inappropriately
  - If the information is no longer needed, get written authorization from your supervisor to have the files moved to storage or destroyed (i.e., shred or burn)

Guidelines for PII/PHI

- Ensure all PII/PHI is protected from casual or unintentional disclosure
  - Use locks, storage rooms, and computer controls
  - Position fax machines and computer screens so they face away from heavy traffic and public access
  - Be aware of surroundings when using a cell phone or Personal Data Assistant (PDA)
  - Lock the computer when away from the desk.
- Follow local policies and procedures for handling PII/PHI

Using and Disclosing PII/PHI

- Disclosing PII/PHI refers to sharing information – verbal, paper, and electronic
- Workforce access and disclosure of PII/PHI for the purposes of treatment, payment, and healthcare operations (TPO) is permitted without signed authorization from the individual
- Some ways to minimize incidental disclosures
  - Do not discuss information in public places
  - Protect computer screen from public view
  - Observe the “Minimum Necessary” Standard when sharing and relating information

Transmitting PII/PHI

- PII/PHI can be transmitted between facilities by methods that include the use of e-mail and fax
  - Before the transmission of PII/PHI, contact your supervisor to ensure the information being sent is encrypted
  - Do not send PII/PHI to unknown sites or facilities
  - Use only DoD authorized information systems, networks, and applications
  - Transmit PII/PHI using remote access only with prior approval
  - Use your CAC to log in and off from your workstation and to encrypt e-mails containing PII/PHI

Transporting PII/PHI

When necessary, PII/PHI can be physically transported between approved locations with a supervisor's authorization, when electronic means are not appropriate

- Obtain authorization from a supervisor before transporting PII/PHI
- Use passwords to protect networks and laptops that contain PII/PHI
- Contact your supervisor to ensure that portable media, including laptops, PDAs, USB portable memory drives, and compact discs (CDs) are encrypted
- Enforce "strong password rules" (alpha/numeric, special characters, and at least 8 characters)
- Do not allow employees to share passwords
- Wrap all PII/PHI in envelopes or wrappings before transporting outside of TMA buildings. Envelopes should be:
  - Opaque
  - Strong and durable
  - Able to prevent unintentional disclosure during transit
  - Clearly marked, including name and destination address
- Ensure there is a tracking process in place for the transportation of PII/PHI, whether in paper records or CDs/media devices; and that accountability be strongly emphasized with the establishment of this process

Storing PII/PHI

- **Storing Paper PII/PHI**
  - Paper storage must be secured under lock and key when unattended
  - Documents must be covered or in folders if there are visitors around the work area
- **Storing Electronic PII/PHI**
  - Ensure your computer has virus protection installed
  - Maintain a record of personnel with access to hardware and software containing PII/PHI
  - Lock unattended laptops
  - Use passwords to protect files and all portable or remote devices
  - Contact your supervisor to ensure the use of encryption on all portable or remote devices, including laptops, thumb drives, PDAs, and CDs *(Please refer to the "Warning" graphic above Section 7 regarding the current policy on the use of portable media in DoD systems)*
  - Do not download PII/PHI onto remote systems or devices without approval

Destroying PII/PHI

- Authorization must be issued *before* deleting or destroying any stored PII/PHI from local file directories, networks, removable devices, or paper files
- PII/PHI that meets the definition of a record, regardless of media, shall be destroyed by the appropriate method in accordance with DoD Administrative Instruction 15, Records Management, and current preservation orders
- PII/PHI that is no longer required for operational purposes must be destroyed completely to prevent recognition or reconstruction of the information
- Non-record PII/PHI may be destroyed at any time. PII/PHI that meets the definition of a record, regardless of media, shall be destroyed by the appropriate method in accordance with DoD Administrative Instruction 15, Records Management, and current preservation orders

Incidents and Breaches

Incident

- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
- The threat can be accidental or deliberate on the part of a user or external influence

Breach

- "Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will adversely affected"

Source: DoD 5400.11-R, "DoD Privacy Program", May 14, 2007

Breaches


EXTRA! EXTRA!

READ ALL ABOUT IT!

Some TRICARE Beneficiary Data Put At Risk

Data for nearly 600,000 households enrolled in TRICARE stored on a government-contractor's unprotected computer server could have been exposed to hackers, defense officials announced today. Beneficiaries' names, addresses, Social Security Numbers, birth dates and some health information was stored on a computer server that was not using a firewall and did not have adequate password protection, TRICARE Management Activity officials said…

- Data breaches continue to make headlines
- With increased use of electronic records comes the vulnerability of data breaches
- A breach can occur with information in paper form
- Responding quickly to a breach is essential in mitigating the possibility of information loss

Lost, Stolen, or Compromised Information

- Examples of Breaches
  - Misdirected fax documents
  - Unsecured mailing or transporting of documents
  - Lost or stolen removable media devices
  - Transmission of unsecured emails and unencrypted files
  - Unauthorized use of another user's account
  - Unauthorized use of system privileges and data extraction
  - Unauthorized release of DoD-sensitive information (SI) and execution of malicious code that destroys DoD SI

Breach Reporting

What Should I Do If a Breach Occurs?	
When a potential or actual loss, theft, or compromise of information occurs, the breach shall be reported as follows:	
TMA Components	***Uniformed Services***
▪ Leadership – **immediately** ▪ TMA Privacy Office – within **1 Hour (PrivacyOfficerMail@tma.osd.mil)** ▪ US CERT* – within **1 Hour** ▪ Defense Privacy Office – within **48 Hours**	▪ Leadership – **immediately** ▪ US CERT – within **1 Hour** ▪ DoD Component Sr. Privacy Officials – within **24 Hours** ▪ TMA Privacy Office – within **24 Hours (PrivacyOfficerMail@tma.osd.mil)** ▪ Defense Privacy Office – within **48 Hours**

Note: If necessary, notify issuing banks if government-issued credit cards are involved, and law enforcement.

*US Computer Emergency Readiness Team

Breach Reporting

- The Breach Report Form should include, but is not limited to:
  - Date of breach
  - Breach discovery date
  - Date reported to US-CERT
  - Total number of individual(s) affected by the breach
  - Type(s) of PII involved

- The POA&M should include, but is not limited to:
  - Actions to mitigate adverse affects
  - Timeline for actions to be taken
  - Actions to prevent recurrence

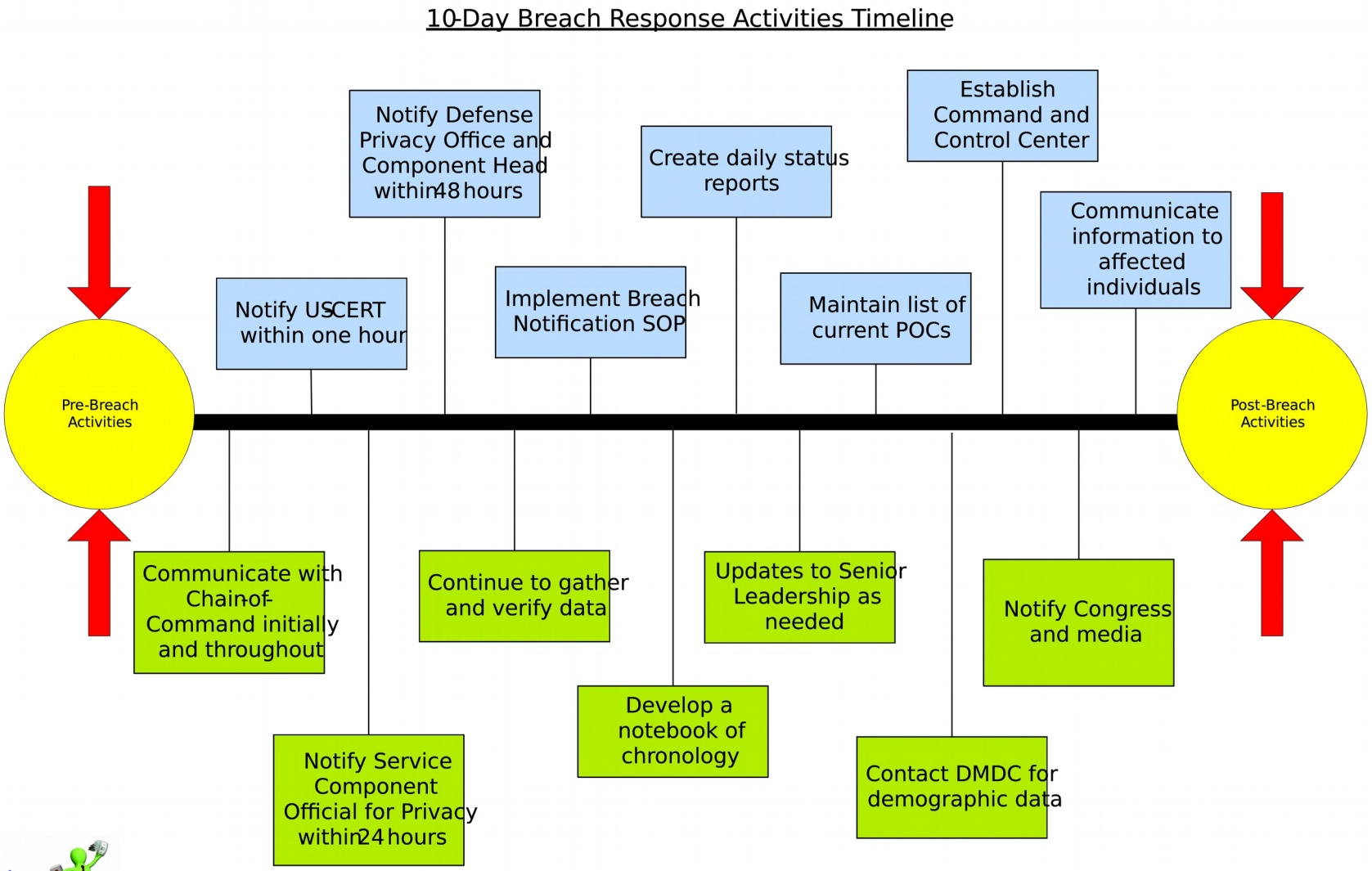
Breach Notification

- Breach Notification
  - Five factors to consider when assessing the likelihood of risk and/or harm:
    1. Nature of the Data Elements Breached
    2. Number of Individuals Affected
    3. Likelihood of the Information is Accessible and Usable
    4. Likelihood the Breach May Lead to Harm
    5. Ability of the Agency to Mitigate the Risk of Harm

Breach Notification

- DoD Components are to thoroughly document the circumstances of all breaches of PII and the decisions made relative to the five factors in reaching their decision to notify or not notify individuals
- When the decision is made to notify, individuals will be notified as soon as possible, but not later than **10 working days** after the breach is discovered and the identities of the individuals are ascertained

Breach Response Time – Example



*Activities are not all inclusive nor in a specific order

Best Practices

Safeguarding Data/Preventing Breaches

- **DO**
  - Remove your Common Access Card (CAC) from your computer to prevent unauthorized access to data
  - Ensure that your notes and working papers that may contain PII/PHI are shredded or put in a burn bag
  - Make certain that filing cabinets are purged of information prior to moving or disposal
  - Verify that e-mail extensions make sense
  - Always use a cover sheet with a confidentiality disclaimer statement when sending faxes

Safeguarding Data/Preventing Breaches

- Avoid clicking on links sent in unsolicited e-mails
- Challenge “anyone” who asks to see PII or PHI for which you are responsible and determine if they have a need to know
- Prevent anyone looking over your shoulder when you are accessing PII/PHI
- Refrain from sharing your passwords/personal identification numbers (PINs) with anyone
- Erase hard drives using prescribed Information Assurance procedures when disposing of equipment

Safeguarding Data/Preventing Breaches

- Ensure proper chain of custody when handling evidence from a breach
- Contain all breaches, whether physical or technical
  - If physical – secure the area
  - If technical – shut down the system
- Secure all breach evidence; safeguard all information involved in the breach

Other Helpful Hints

The TMA Privacy Office Web site has many resources

www.tricare.mil/tmaprivacy/

- In particular
  - Section on Compliance Assist Visits (Resources)
    - Compliance Assist Visits Self-Assessment Guide
    - Supplement

Summary

- Safeguarding electronic health records helps to ensure that the PHI of the 9.2 million TMA beneficiaries is well protected
- DoD and Federal guidelines are in place to protect health information
- MHS employees must follow these guidelines to prevent the theft, loss, or compromise of this information
- Privacy and Security is everyone's responsibility

Privacy Office Contact Information

If you have any questions or concerns, please contact the

Privacy Office

TMA Privacy Office
Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA 22041

Privacymail@tma.osd.mil